Final Project: Encryption

1 Description of the project

Summary

For this project, you will

1. Choose a plaintext of at least 50 characters and encrypt it using
   (a) A shift (Caesar) cipher with your choice of shift;
   (b) A transposition cipher with a key of your choice, of at least 5 letters;
   (c) a Vigenère cipher, using the same key;
   (d) a two-step encryption system that you create ("Your Encryption Method"), described in the next section.
2. Then you will write out careful instructions for decrypting a message using your 2-step system and test these instructions out on a friend, by seeing if they can successfully decrypt the plaintext that you encrypted using Your Encryption Method.
3. Finally, you will analyze Your Encryption Method.

Creating a 2-step Encryption System

1. **Create an encryption system that involves at least 2 steps**. Here are the requirements:
   (a) One step must be a **substitution cipher**, meaning that you are replacing the characters in your message with different characters, following some established mapping (such as an alphanumeric Caesar cipher with a given shift).
   (b) One step must be a **transposition cipher**, meaning that you are changing the order of characters to obscure the message (such as tabular transposition).
   (c) You need to use a different substitution cipher and transposition keyword than you use in other parts of this project.
   (d) Each step need to be **reversible**, meaning that you can write down a step-by-step process to decrypt a message.
2. Give your encryption system a name.
3. Write out an explanation of both encryption steps. Use words and terms that someone **who is not in the class** can understand.
4. Write out a step-by-step guide for decrypting a message with your system. Use words and terms that someone **who is not in the class** would be able to understand and apply.

Further Analysis

1. **Test your decryption instructions with a friend** by providing your decryption instructions and your ciphertext that was encrypted using Your Encryption Method.

2. **Answer each of the following questions:**
   (a) How did your friend do? Were your decryption instructions clear enough?
   (b) How hard do you think it would be for someone to decrypt these messages without knowing your encryption process? Is your encryption system secure?

2 Project Deliverables

How to submit

- Your project must have a **Title Page**, containing your name and which project you are completing.
- Your final project must be submitted in class during the final exam period. (Note that you can print out materials at the Student Success Center!)
- Your final project must be typed.
- You should use sentences to describe what each piece of your project is doing and what you are computing: one of your classmates should be able to read your project and understand what you are doing.
- Your final project must be stapled.

What to submit

Your final project must contain the following sections. Each section should start on a separate page.

- A section titled **My Encryption Method** containing:
  - The name of your encryption system
  - A step-by-step guide for **encrypting** a message with your system, clearly explaining how both steps work
  - A clear, step-by-step guide for **decrypting** a message with your system, that is understandable by someone who is not taking/has not taken Math F113X
- A section titled **Encrypted Messages** containing:
  - Your plaintext
  - Your plaintext encrypted using a shift cipher. You must clearly say what shift you are using. **Prohibited shifts**: 0 ($A \to A$), 1 ($A \to B$) and -1 ($A \to Z$).
  - A choice of keyword of at least 5 letters.
  - Your plaintext encrypted using a transposition cipher using your keyword. Include supporting work for the encryption.
  - Your plaintext encrypted using a Vigenère cipher using your keyword. Include supporting work for the encryption.

  - Your plaintext encrypted using Your Encryption Method. Include supporting work for the encryption.

- A section titled **Further Analysis** containing

  1. Your answer to the question:

     "How did your friend do? Were your decryption instructions clear enough?"

     This should include answers to the following:

     (a) A description of your process of getting your friend to do the decryption (what happened?)

     (b) Whether or not your friend successfully decrypted your plaintext using the step-by-step decryption guide.

     (c) How long it took

     (d) An assessment of the clarity of your decryption guide and how it might need to be improved

  2. Your answer to the question:

     "How hard do you think it would be for someone to decrypt these messages without knowing your encryption process? Is your encryption system secure?"

     You should address the following:

     (a) Talk about at least one strength of your encryption system that would make it difficult to hack

     (b) Talk about at least one possible weakness of your encryption system that may make it vulnerable to hacking

     (c) Give an overall assessment of the security of your encryption system

  These answers should be written in complete sentences, and they should fully explain your answer to the questions, with justification.

3 Grading

Your project will be graded out of 100 points using the following rubric:

1. **My encryption system** (15 points)

   (a) Substitution described clearly

   (b) Transposition described clearly, including a key word and its use

   (c) Named encryption system

   (d) Clear encryption instructions provided that is understandable by someone who is not in Math F113X

2. **Encrypted messages** (25 points)

(a) The plaintext, shift, and keyword used are clear

(b) Plaintext was correctly encrypted using the shift cipher

(c) Plaintext was correctly encrypted using a transposition cipher, with supporting work

(d) Plaintext was correctly encrypted using a Vigenère cipher, with supporting work

(e) Plaintext was correctly encrypted using Your Encryption Method, with supporting work

3. **Decryption check** (10 points)

   (a) A clear step-by-step guide for decrypting messages was provided

   (b) The guide is understandable by someone who is not in Math F113X

4. **How did your friend do?** (20 points)

   (a) Clear explanation of whether or not your friend successfully decrypted your plaintext using the step-by-step decryption guide.

   (b) Stated how long it took your friend to decrypt your messages

   (c) Provided assessment of the clarity of the step-by-step decryption guide and described how it could be improved.

5. **Answer to "How hard do you think it would be for someone to decrypt these messages..."** (20 pts)

   (a) Analyzed Your Encryption System

   (b) Discussed least one strength of Your Encryption System that would make it difficult to hack

   (c) Discussed of at least one possible weakness of Your Encryption System that may make it vulnerable to hacking

   (d) Overall assessment of the security of Your Encryption System

6. **Grammar, mechanics, and following directions** (10 points)

   - Used sufficient words and **complete sentences** in your discussions
   - Used correct grammar and mechanics in your writing
   - Used words and headings to make it clear what you are answering where
   - Computations are presented clearly and legibly
   - Followed the directions